Standardized
E-Gas Monitoring Concept for Gasoline and Diesel Engine Control Units

Version 5.5

1 General Part 4

1.1 Participants in the Working Group 4

2 Introduction 4

3 Definition of Terms 4

4 Abbreviations 6

5 Developing Guidelines and Basic Principles 7

6 Amendments / References 7

7 System Definition 8

8 Hazard Analysis and Risk Assessment 9

9 Functional Safety Concept 10

10 Technical Safety Concept 13

10.1 3-Level Monitoring Concept 13

10.1.1 System Overview Electronic Control Unit (ECU) 13

10.1.2 ECU Functions and Component Monitoring of Level 1 14

10.1.2.1 Characteristic and Diagnostic Requirements of the Throttle-Valve Actuator 16

10.1.2.1.1 Characteristic of the Throttle-Valve Sensor Technology 16

10.1.2.1.2 Fault Detection 16

10.1.2.2 Design Characteristics and Diagnostic Requirements of the Pedal Value Sensor 17

10.1.2.2.1 Design Characteristics of the Pedal Value Sensors 17

10.1.2.2.2 Design Characteristic of the ECU Input Wiring (Analog Sensor) 17

10.1.2.2.3 Design Characteristic of the Signal Content with Digital Communication Protocol (e.g. SENT) 17

10.1.2.2.4 Design Characteristics of the ECU for Evaluation of the Digital Transmission Protocol (e.g. SENT) 17

10.1.2.2.5 Fault Detection 17

10.1.2.3 Determination of the Required Pedal Value of Level 1 in Normal Operation 18

10.1.2.4 Accelerator Pedal / Brake Plausibility 18

10.1.3 General Requirements of Level 2 Function Monitoring 19

10.1.3.1 Inclusion of the torque loss of level 1 for “permissible torque” calculation 25

10.1.3.2 Taking over Adaptation Values / Correction Factors from Level 1 to Level 2 (Tolerance limitation) 25

10.1.3.3 Monitoring of the Injection Output Variables from Level 1 26

10.1.3.4 Monitoring of the Trigger Output Unit (e.g. TPU, PCP) 26
10.1.3.5 Continuous Torque Monitoring Diesel (Torque Comparison), Reverse Calculation of Current Torque Level 2 26
10.1.3.5.1 Rail Pressure Monitoring 26
10.1.3.5.2 Torque Relevant Efficiencies of Injection Quantities 27
10.1.3.5.3 More Torque Relevant Efficiencies (e.g. Air Influence) 27
10.1.3.6 Continuous Diesel Monitoring (Acceleration Comparison) 28
10.1.3.6.1 Level 1 Requirements 28
10.1.3.6.2 Level 2 Requirements 29
10.1.3.7 Continuous Diesel Monitoring, Overrun Monitoring 30
10.1.4 Validation of the Torque Measurement in the ECU Network 30
10.1.5 Level 3 Controller Monitoring 30
10.1.5.1 Monitoring of the Q&A Communication 31
10.1.5.1.1 Monitoring with L3_MM 31
10.1.5.1.2 Monitoring with L3_SW of the Function Controller 31
10.1.5.2 Iteration Rate of the Q&A Communication 31
10.1.5.3 Test Paths of the L3_SW of the Function Controller 31
10.1.5.4 Question Generating of the Monitoring Module L3_MM 32
10.1.5.5 TPU Monitoring 32
10.1.5.6 Shutoff Path Test 33
10.1.5.7 A/D Converter Test 33
10.1.5.8 Reset System Behavior 33
10.1.5.9 Diagram of the Level 3 Fault Reactions 34
10.2 System Fault Reactions 35
10.3 Additional Technical Requirements 35
10.3.1 Safe Engine Stop 35
11 Appendix: Fault Reactions 36
11.1 Level 1 Monitoring Faults 36
11.1.1 Pedal Value Sensor 36
12 List of Figures 48

EGAS_e-1

1 General Part

EGAS_e-2

1.1 Participants in the Working Group

Company	Repres.
Audi AG	Mr. Nägler
BMW AG	Mr. Ertl
BMW AG	Dr. Möllmann
Daimler AG	Mr. Rehm
Porsche AG	Mr. Staib
VW AG	Mr. Veldten

EGAS_e-3

EGAS_e-5

2 Introduction

Drive-by-Wire-Systems are now state-of-the-art technology for control gasoline and diesel engines.

EGAS_e-6 The high conditions on these systems and the integration into networked vehicle systems requires a closely monitoring of their functionalities.

EGAS_e-7 The automotive manufacturers represented in the EGAS working group see no potential of brand-name differentiation in solving this mission.

EGAS_e-8 For this reason, they have agreed to standardize the monitoring concept for EGAS systems and implement this concept into the engine control systems of their vehicles, supplier-independent.

EGAS_e-9 Despite of functional differences between the engine control of gasoline and diesel engines, which mainly concern different working procedures, the EGAS working group considers that it is possible to standardize monitoring core components and functions

EGAS_e-10 The available documentation describes the principles of the concept that shall be used.

EGAS_e-11 It is intended to be used as a guideline for the development of future engine control systems.

EGAS_e-12 The EGAS monitoring concept used in the present document has been developed by the supplier comprehensive EGAS working group in collaboration with control unit manufacturers.

EGAS_e-15 When using this specification, the license rights shall be cleared by the concerned legal and patent departments.

EGAS_e-16

3 Definition of Terms

EGAS_e-17
- A **driving cycle** shall be the operation time between the key initiated engine start / stop, inclusive a possible power latch time duration of the engine control unit.

EGAS_e-18
- An **error or a single error** shall be the non-fulfillment of at least one requirement regarding a required characteristic of the considered unit.

EGAS_e-19
- An **error** shall be defined as latent, if it is not detected in the next driving cycle, either by the electronic engine control unit or by the driver.

EGAS_e-20
- A **double error** shall define two errors, which occur within a short period („simultaneous“) and they do not have any causal connection.

EGAS_e-21
- A **dual error** shall define two single errors, which occur beyond a short period and they do not have any causal connection.

EGAS_e-22
- The **fault detection** shall be defined as the identification of exceeding permissible deviations of relevant system parameters leading to a non-fulfillment of at least one requirement regarding a required characteristic of a considered unit. An error shall be defined as detected if the detection time is sufficient to avert or reduce the error effect (severity).

EGAS_e-23
- The **failure effect** shall define the deviation of the system behavior in a faulty condition to the system behavior in a fault-free condition. (Compliance of the requirements to relevant system parameters).

EGAS_e-24
- The **failure reaction** is the completeness of all initiated measures after the error detection, in order to reduce the failure effect to a permissible limit.

EGAS_e-25
- **Controllable failure reactions** in the case of a fault characterized as:

EGAS_e-26
  - defined released reaction times

EGAS_e-27
  - defined released limitations of engine torque, engine speed or acceleration

EGAS_e-28
- **„Raw signals"** of control units are:

EGAS_e-29
  - Sampled digital or analog signals of the HW input register.

EGAS_e-30
  - current and not modified input data received by data bus.

EGAS_e-31
- **Reset** refers to setting the systems in a controlled state.

  This shall be triggered by a SW function call or a HW mechanism of the engine control unit (ECU):

EGAS_e-32
  - SW reset: initiated by a function call (ROM-, RAM test, etc.)

EGAS_e-33
  - HW reset: initiated by hardware measures (watchdog, power-on reset, etc.)

EGAS_e-34
- The **injection cut off** (ICO) limits maximum authorized engine rotational speed (e.g. by cut off of the torque relevant injections).

EGAS_e-35
- The **Pedal Value Sensor** (PVS) measures the position of the accelerator pedal and thereby the driver´s demand.

EGAS_e-36
- The **Timing Processing Unit** (TPU) or other comparable co/sub processors with time or angle synchronous inputs and outputs.
  These are relevant for the torque acquisition or torque conversion (e.g. speed measurement, actuating the injection and spark output stages).

EGAS_e-37

4 Abbreviations

Abbr. in E.	English
ADC	**A**nalog **D**igital **C**onverter
AJD	**A**ctive **J**erk **D**amper
ASIC	**A**pplication **S**pecific **I**ntegrated **C**ircuit
SS	Stop light Switch
BTS	**B**rake **T**est **S**witch
CAN	**C**ontroller **A**rea **N**etwork
CR	**C**ommon **R**ail
TVDV	Throttle Valve Default Value
TV	Throttle Valve
TV1	Throttle Valve Angle from real Value **1**
TV2	Throttle Valve Angle from real Value **2**
L3_SW	Level 3 Monitoring Software in the Function Controller
L3_MM	**L**evel 3 **M**onitoring **M**odule
ICO	**I**njection **C**ut **O**ff
CC	**C**ruise **C**ontrol
FMEA	**F**ailure **M**ode & **E**ffect **A**nalysis
FC	**F**unction **C**ontroller
HW	**H**ard**w**are
AV	**A**ctual **V**alue
ID	Idle
EDTC	**E**ngine **D**rag **T**orque **C**ontrol
n_mot	Engine Speed
PFC	**P**rogram **F**low **C**hecks
PVS	**P**edal **V**alue **S**ensor
CU	**C**ontrol **U**nit
SRC	**S**ignal **R**ange **C**heck
SW	**S**oft**w**are
TPU	**T**iming **P**rocessing **U**nit or comparable co/sub processor e.g. PCP
MM	**M**onitoring **M**odule

EGAS_e-38

EGAS_e-39

5 Developing Guidelines and Basic Principles

EGAS_e-40
- Protection of life has the highest priority.

EGAS_e-41
- Reliability has higher priority than backup functions.

EGAS_e-42
- The monitoring shall be independent of the engine concept and as far as possible independent of the driver reaction.

EGAS_e-43
- Functions, in particular for system monitoring (also error reactions), shall be easy and manageable.

EGAS_e-44
- The system shall be designed so that single errors and single errors in combination with latent errors lead to controllable system reactions. The corresponding signal paths (sensors, actuators, functions) shall be monitored.

EGAS_e-45
- The system shall be designed so that double and dual faults lead to controllable system reaction as required as state-of-the-art.

EGAS_e-46
- In terms of a high system availability, staged error reactions shall be strived.

EGAS_e-47
- A signal path shall be classified as „confirmed defected“ after an explicit detection (e.g. after debouncing event or time) and before the reaction shall be activated. Previously the defect shall be classified as „assumed defected“.

EGAS_e-48
- Appropriate reaction mechanisms shall be defined according to the function in the case of an "assumed defect" and „confirmed defect“.

EGAS_e-49
- The reset of fault reactions shall be determined in individual cases and shall be performed controllable. Non-continuous transitions shall be avoided.

EGAS_e-50
- Engine stop is permitted when no other controllable system reaction can be ensured.

EGAS_e-51
- The transmitter is the responsible for the content of its initiated messages at the control unit interface. This means that, e.g. external torque requests by the transmitting control unit shall be secured. The transmission path and the actuality of the messages shall be checked by the engine control system.

EGAS_e-52
- If errors happen in combination with the subsequent single errors cause unintended system reactions, the driver should be informed. (optically or by modifying the driving behavior).

EGAS_e-53
- The monitoring of the function controller must be kept robust and simple. This includes a possible implementation with an ASIC.

EGAS_e-54
- The effectiveness of the redundant shutoff paths shall be tested in each driving cycle.

EGAS_e-55
- Shutoff paths of the monitoring concept shall be robust if a defect power supply drifts. The power supply concept shall be monitored to avoid possible damages of components. Controllable failure reactions shall be initiated.

EGAS_e-56
- The technical safety concept shall be implemented in accordance with the requirements of ISO 26262.

EGAS_e-57

6 Amendments / References

EGAS_e-60

ISO 26262, First Edition 2011-11-15

EGAS_e-61

7 System Definition

EGAS_e-62 Compliance to ISO 26262 requires the definition of the system scope (item definition).

EGAS_e-63 Subject of consideration shall be an internal combustion engine as part of the powertrain of a road vehicle where the powertrain is directly coupled to the drive wheels in the case of a closed powertrain.

EGAS_e-64 The next functional characteristics shall be assigned to the combustion engine:

EGAS_e-65
- Providing driving torque

EGAS_e-66
- Providing braking torque by means of drag torque of the combustion engine

EGAS_e-67 Application environment:

EGAS_e-68
- Passenger cars

EGAS_e-69 Structure:

EGAS_e-70
- The internal combustion engine shall be the single source of driving torque of the vehicle.

EGAS_e-71
- The combustion engine shall be coupled directly to the drive wheels by a closed power train.

EGAS_e-72
- The combustion engine shall be controlled by the engine ECU.

EGAS_e-73 Now an example of a schematic electronic architecture for controlling a gasoline engine can be considered. (the application to other combustion engines e.g. diesel shall be assumed).

EGAS_e-74 An engine control system for gasoline engine regarding the EGAS-content consists of the following components (fig.: 1):

EGAS_e-75
- Accelerator pedal

EGAS_e-76
- Engine control unit

EGAS_e-77
- Throttle-valve

EGAS_e-78

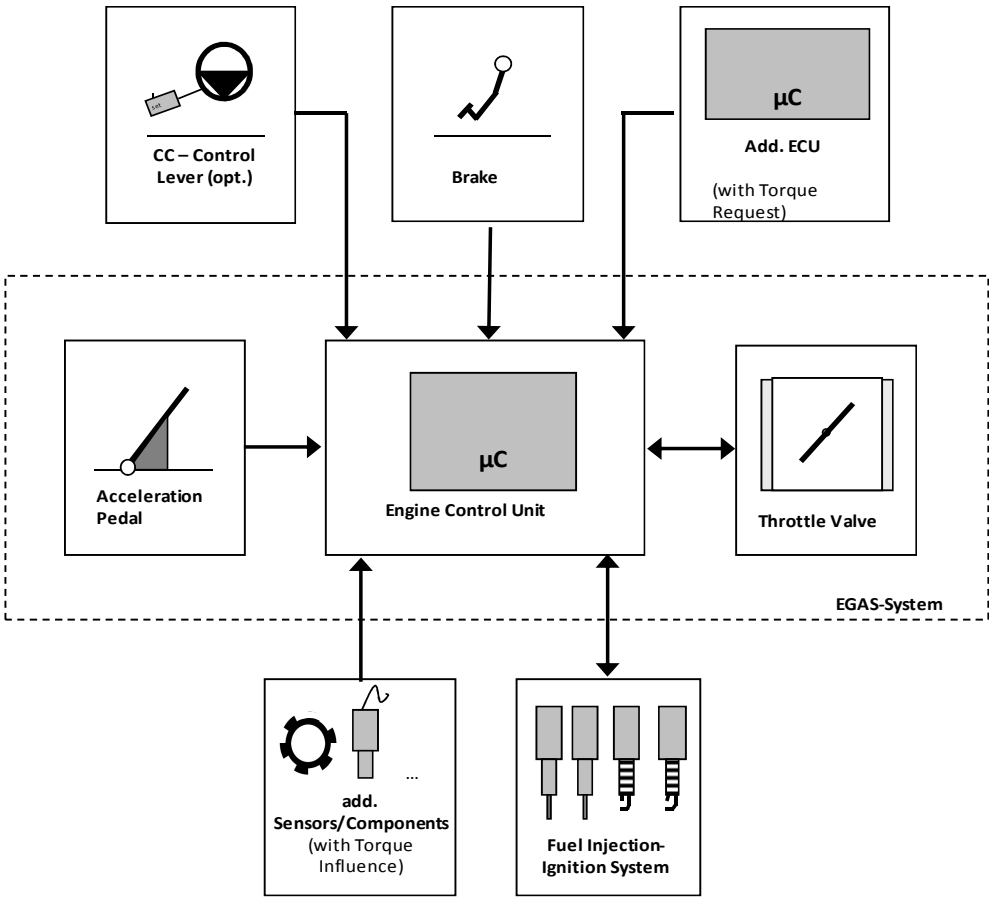


Figure 1 Overview of the ETC system with interfaces (simplified example of a gasoline engine)

EGAS_e-79 Additional interfaces, which may affect the providing of the driving torque shall be considered.

EGAS_e-80

8 Hazard Analysis and Risk Assessment

EGAS_e-81 Based on the system definition described in the previous chapter, the system behavior in typical driving conditions was analyzed in the scope of a hazard analysis and risk assessment and the hazards caused by errors in the EGAS system were determined.

EGAS_e-82 The following safety goals shall be defined as a result of the hazard analysis and risk assessment:

EGAS_e-83 SZ-01 Prevention of unintended acceleration → ASIL B

EGAS_e-84 SZ-02 Prevention of missing acceleration → QM

EGAS_e-85 SZ-03 Prevention of unintended deceleration → QM

EGAS_e-86 SZ-04 Prevention of missing deceleration → QM

EGAS_e-87 Therefore, due to safety goal SZ-01, a monitoring concept shall be required that detects “unintended acceleration” and transfers the vehicle into a controllable and safe state within an appropriate fault tolerance time. (ftt)

EGAS_e-88 The safety goals SZ-02 to SZ-04 represent the controllable conditions and therefore are not subject of consideration.

EGAS_e-89 The OEM internal analyses shall provide as a foundation, e.g. from accident research and a statement from TÜV SÜD (2006).

EGAS_e-90 The next chapters describe in detail the essential safety requirements to achieve the safety goal SZ-01, “unintended acceleration”.

These requirements shall be implemented according to ASIL B.

EGAS_e-91

9 Functional Safety Concept

EGAS_e-92 An Invalid vehicle acceleration occurs in systems with only one torque source and propulsion engine respectively only due to a faulty torque demand / torque conversion.

The safety goal SZ-01 shall be achieved by a functional safety concept.

EGAS_e-93 This concept shall monitor the permitted vehicle acceleration, respectively the permitted driving torque to bring the vehicle into a safe controllable state within an adequate fault-tolerance time.

EGAS_e-94 The safety requirements are distributed to the following components:

- Sensors (S1/S2)

  EGAS_e-95 A plausibility check can be applied to the sensor signals (e.g. driver accelerator pedal demand) after capturing the signals.

- EGAS_e-96 Actuators (A)
  A plausibility check can be applied to the actuator signals (e.g. throttle position) after capturing the signals.

- Engine control unit (L)
  - The engine control unit detects sensor faults.
  - The engine control unit detects actuator faults.
  - EGAS_e-97 A safety concept is implemented in the engine control unit, which validates and detects a not permissible exceeding driving torque. The system fault reaction shall result in a safe state.
  - The safety concept is based on the idea of a centralized functional monitoring architecture. (level 2).

EGAS_e-98

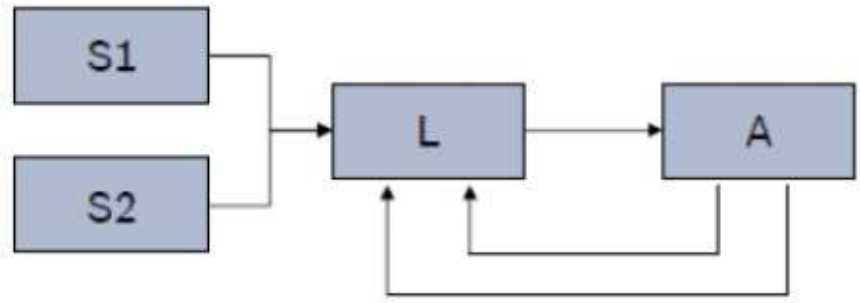


Figure 2 Safety block diagram

EGAS_e-99 Central functional monitoring:

EGAS_e-100 The functional monitoring level (level 2) shall calculate and monitor functions independently of the functional level (level 1). In case of an error detection, a controllable (safe) state has to be adjusted.

EGAS_e-101 An independent development ensures that systematic errors do not have the same effect on the functional level (level 1) and on the monitoring level (level 2).

EGAS_e-102 Additional measures shall be implemented into the control unit to verify the integrity of the applied ECU HW.

It shall be ensured that errors which are located in level 1 and in the ECU-HW cannot have an undetected influence to level 2.

EGAS_e-103 Allocation of the safety requirements to the engine control unit:

EGAS_e-104 The next table contains the reference to the sections in the technical safety concept. The safety requirements of this concept are specified more in detail.

No

SANF-01

Safety requirement for SZ-01:

Sensors shall be designed so that they can be checked for plausibility

EGAS_e-105 **Component:**

Driver Accelerator Pedal

Technical implementation:

10.1.2.2.1

10.1.2.2.3

No

SANF-02

Safety requirement for SZ-01:

EGAS_e-106 Sensors shall be designed so that they can be checked for plausibility

Component:

Throttle-valve actuator1)

Technical implementation:

10.1.2.1.1

No

SANF-03

Safety requirement for SZ-01:

The engine control unit detects sensor faults (e.g. accelerator pedal, throttle-valve, brake, cruise control lever2), additional torque relevant sensors / components) by using appropriate plausibility checks.

Component:

EGAS_e-107 Engine control unit

Technical implementation:

10.1.2
10.1.2.1.2

10.1.2.2.2
10.1.2.2.4
10.1.2.2.5

10.1.2.3

10.1.2.4

No

SANF-04

Safety requirement for SZ-01:

EGAS_e-108 Torque requests of other control devices that are transmitted by networks shall be checked for plausibility (e.g. accelerator pedal, throttle-valve, brake, CC-control lever2) in the engine controller

Component:

Engine control unit

Technical implementation:

10.1.2

No

SANF-05

EGAS_e-109 The engine control unit detects actuator errors (e.g. throttle-valve1), fuel quantity) by using appropriate plausibility checks)

Component:

Engine control unit

Technical implementation:

10.1.2

No

SANF-06

Safety requirement for SZ-01:

In the engine control unit a safety concept shall be implemented for validation and confirmation of a not permissible exceeding driving torque or an unintended acceleration.

EGAS_e-110 In case of a fault the engine control unit shall switch to a safe state.

Component:

Engine control unit

Technical implementation:

10.1.3

10.2

10.3

No

SANF-07

Safety requirement for SZ-01:

EGAS_e-111 The function controller shall be monitored

Component:

Engine control unit

Technical implementation:

10.1.5 ff

EGAS_e-112 *[1)]Only applies to gasoline engines in air-measured based systems.*

EGAS_e-113 *[2)]Project specific*

EGAS_e-114

10 Technical Safety Concept

EGAS_e-115

10.1 3-Level Monitoring Concept

EGAS_e-116

10.1.1 System Overview Electronic Control Unit (ECU)

EGAS_e-117 The monitoring concept shall be designed in 3 levels:

EGAS_e-118 **Level 1**

EGAS_e-119 It is referred as **functional level**.

EGAS_e-120 Level 1 contains the engine control functions, i.a. implementation of the requested engine torque, component monitoring, input / output variable diagnostic and to control the system reactions if a fault shall be detected.

EGAS_e-121 **Level 2**

EGAS_e-122 It is referred as **function monitoring level**.

EGAS_e-123 Level 2 detects the defective process of level 1 functional software, e.g., by monitoring the calculated torque values or the vehicle acceleration. In case of fault, system reactions are triggered.

EGAS_e-124 **Level 3**

EGAS_e-125 It is referred as **controller monitoring level**.

EGAS_e-126 The monitoring module shall be an independent part of the function controller (e.g. ASIC or controller), which tests the correctly executed program during the question-answer process.

EGAS_e-127 In case of fault, system reactions are triggered independently of the function controller

EGAS_e-128

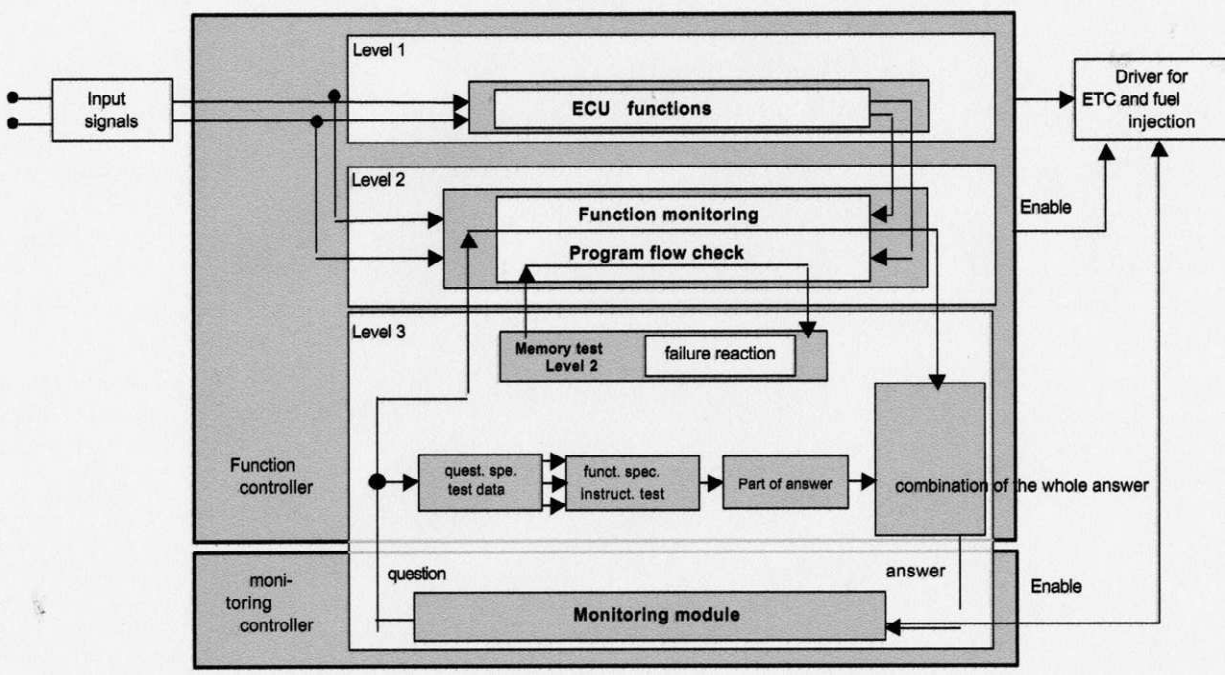


Figure 3 System overview; 3 level concept

EGAS_e-129

10.1.2 ECU Functions and Component Monitoring of Level 1

EGAS_e-130 Level 1 consists of:

EGAS_e-131
- all engine control functions

EGAS_e-132
- the diagnostic of input and output variables related to monitoring

EGAS_e-133 Only components shall be considered now, which are relevant for monitoring and inherently present in the system. Implying that if a value cannot be directly monitored (according to the state-of-the-art), monitoring another physically correlated values may be also acceptable.

EGAS_e-134 **Sensor component**

EGAS_e-135	♦ Pedal value sensor	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-136	♦ Brake switch	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-137	♦ Engine speed signal	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-138	♦ Load signal	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-139	♦ Lambda oxygen sensor	Gasoline-Direct Injection
EGAS_e-140	♦ Common rail pressure sensor	Gasoline-Direct Injection Diesel-Torque Monitoring

EGAS_e-141	♦ Engine temperature sensor	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring

EGAS_e-142 **Actuator components:**

EGAS_e-143	♦ Throttle valve[1]) *Note:* *[1]) if decisive for the air path*	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-144	♦ Fuel injection cut-off	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-145	♦ Common rail pressure control valve *Note:* *[3]) for CR systems with two actuator concept only*	Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-146	♦ Metering unit *Note:* *[4]) for CR systems only*	Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring

EGAS_e-147 **Signals from other control units**

EGAS_e-148	♦ Received requests that increase torque (signal transmission and currentness) [2]) *Note:* *[2]) torque-increasing requests shall be guaranteed by the sending control unit*	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-149	♦ Vehicle acceleration (if applicable from vehicle speed)	Diesel-Acceleration Monitoring

EGAS_e-150 **Protected shutoff paths of the cruise control**

EGAS_e-151	Brake information	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring

EGAS_e-152 **10.1.2.1 Characteristic and Diagnostic Requirements of the Throttle-Valve Actuator**

EGAS_e-153 ***10.1.2.1.1 Characteristic of the Throttle-Valve Sensor Technology***

EGAS_e-154
- Double sensor with physically separated signal paths

EGAS_e-155
- High diagnostic sensitivity over the complete adjustable range. Current standard shall be a version with characteristic curve progression in the opposite direction and the same voltage swing.

EGAS_e-156
- High resolution for good control precision and diagnostic

EGAS_e-157
- Minor synchronism deviation for effective diagnostic

EGAS_e-158
- Minor drift in environmental and durability conditions (maintain diagnostic limits)

EGAS_e-159 ***10.1.2.1.2 Fault Detection***

EGAS_e-160
- Short-circuits, parallel connections and open-circuit at the throttle valve sensors (including sensor power supply)

EGAS_e-161
- Short-circuits and open-circuits at the throttle valve drive.

fault description:

EGAS_e-162 Voltage offset voltage supply or sensor ground

possible fault detection:

Signal-range-check or synchronism diagnostic sensor 1 to sensor 2

fault description:

EGAS_e-163 Voltage offset sensor 1 or sensor 2

possible fault detection:

Signal-range-check or synchronism diagnostic sensor 1 to sensor 2

fault description:

EGAS_e-164 Short-circuit sensor 1 to sensor 2

possible fault detection:

Position diagnostic (target/current value) or position adjust. diagnostic. (input variable)

fault description:

EGAS_e-165 fault at the actuator

Possible fault detection:

Position diagnostic (target/current value) or position adjust. diagnostic. (input variable)

EGAS_e-166

10.1.2.2 Design Characteristics and Diagnostic Requirements of the Pedal Value Sensor

EGAS_e-167

10.1.2.2.1 Design Characteristics of the Pedal Value Sensors

EGAS_e-168
- Double sensor with physically separated signal paths

EGAS_e-169
- Diagnosable sensor power supply or two sensor power supplies

EGAS_e-170
- Two up to the control unit separated ground paths

EGAS_e-171
- Clear plausibility over the complete adjustable range. Current standard shall be a version with variable-slope increasing performances curves.

EGAS_e-172
- Minor synchronism deviation and sufficient resolution for effective diagnostic

EGAS_e-173
- Minor drift on environmental and durability conditions (maintain diagnostic limits, short pedal dead band)

EGAS_e-174

10.1.2.2.2 Design Characteristic of the ECU Input Wiring (Analog Sensor)

EGAS_e-175
- In case of line breaks, the sensor input circuits shall be dimensioned for voltage level < idling detection threshold.

EGAS_e-176

10.1.2.2.3 Design Characteristic of the Signal Content with Digital Communication Protocol (e.g. SENT)

EGAS_e-177
- Sensor internally detected faults shall be detectable by the receiver, e.g. transmission of an fault code “FF”

EGAS_e-178
- Transmission of a sender identification

EGAS_e-179
- The receiver shall evaluate the currentness of the message, e.g. transmission of a live detection using message counter.

EGAS_e-180
- Checksum transfer

EGAS_e-181

10.1.2.2.4 Design Characteristics of the ECU for Evaluation of the Digital Transmission Protocol (e.g. SENT)

EGAS_e-182
- The complete message content: data signal, message counter, checksums, sender identification, .. shall be available as raw signals for the monitoring level (level 2)

EGAS_e-183

10.1.2.2.5 Fault Detection

EGAS_e-184
- Short-circuits, parallel connections and open-circuits on the driving pedal value sensors (including sensor power supply)

EGAS_e-185 **fault description:**

Potential offset of the voltage supply

possible fault detection:

Synchronism diagnostic sensor 1 to sensor2 or reverse reading of the sensor power supply

EGAS_e-186 **fault description:**

Potential offset sensor 1 or sensor 2

possible fault detection:

Signal-range-check or synchronism diagnostic sensor 1 to sensor 2

EGAS_e-187 **fault description:**

Short-circuit sensor 1 to sensor 2

possible fault detection:

Synchronism diagnostic sensor 1 to sensor 2 or signal-range-check

EGAS_e-188 **fault description:**

Potential offset sensor ground 1 or Sensor ground 2

possible fault detection:

Synchronism diagnostic sensor 1 to sensor 2 or signal-range-check

EGAS_e-189 **fault description:**

missing signal message*

possible fault detection:

Input signal diagnostic test or live detection test

EGAS_e-190 **fault description:**

Outdated message signal*

possible fault detection:

Live detection test

EGAS_e-191 **fault description:**

Inconsistent signal message*

possible fault detection:

Checksum verification

EGAS_e-192 **fault description:**

Message from wrong signal transmitter*

possible fault detection:

Transmitter identification verification or checksum verification

EGAS_e-193 *Protocols for digital signal (e.g. SENT)

EGAS_e-194 #### 10.1.2.3 Determination of the Required Pedal Value of Level 1 in Normal Operation

EGAS_e-195 The sensor characteristic curve of channel 2 initially shall be normalized to the characteristic curve of sensor 1.

EGAS_e-196 The calculation of the required pedal value of level 1 in normal operation shall be performed by a minimum selection of the two sensor channels

EGAS_e-197 #### 10.1.2.4 Accelerator Pedal / Brake Plausibility

A reduction of the propulsion power to a controllable maximum limit shall be performed,

EGAS_e-198 if the driver requests a propulsion power by the accelerator pedal and operates the service brake with a minimum pedal force while the vehicle is moving.

EGAS_e-199 An adequate monitoring of the brake signal input shall be required.

EGAS_e-202

10.1.3 General Requirements of Level 2 Function Monitoring

EGAS_e-203 The level 2 (function controller component) contains:

EGAS_e-204 Monitoring of the performance regulating functions of level 1.

Central part of level 2 for systems with torque monitoring shall be the comparison between a separately calculated “permissible engine-torque” and a “current engine-torque”.

EGAS_e-205

Central part of level 2 for systems with acceleration monitoring shall be the comparison between a separately calculated “permissible vehicle acceleration” and a “current vehicle acceleration”

EGAS_e-206
- monitoring of level 1 fault reaction, if L2 cannot generate separately a fault reaction.

EGAS_e-207
- Level 2 storage areas shall be monitored cyclically

EGAS_e-208
- Calculations for the program flow control

EGAS_e-209 Graphic charts for:

EGAS_e-210
- Gasoline manifold injection

EGAS_e-211

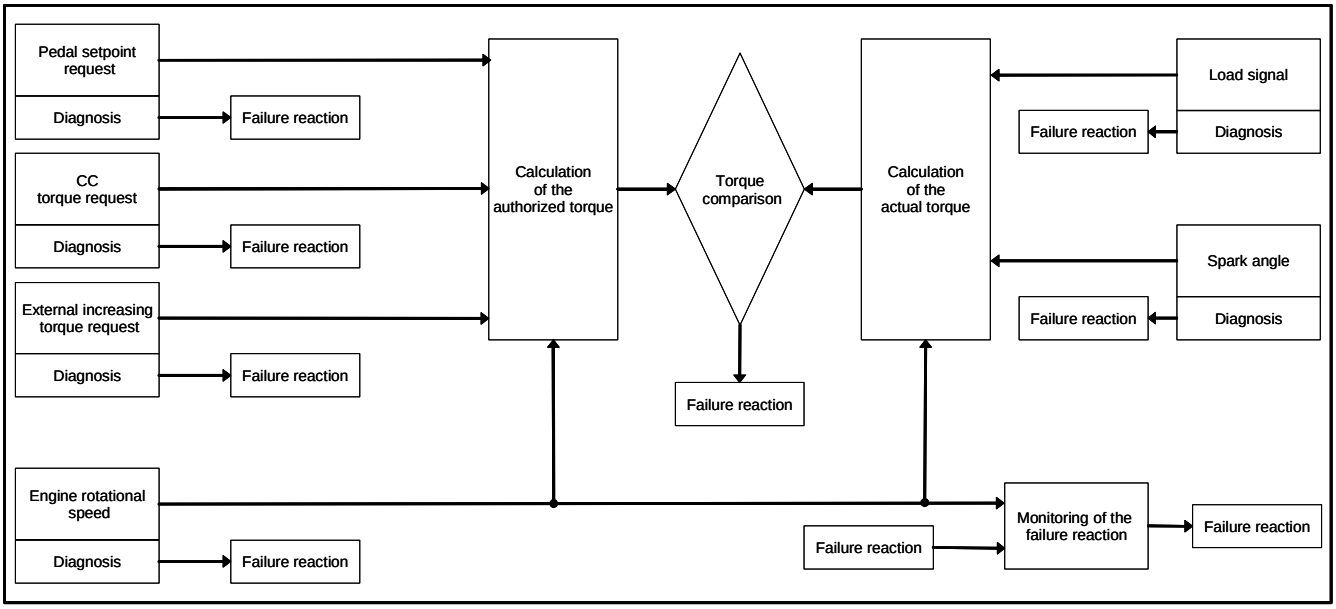
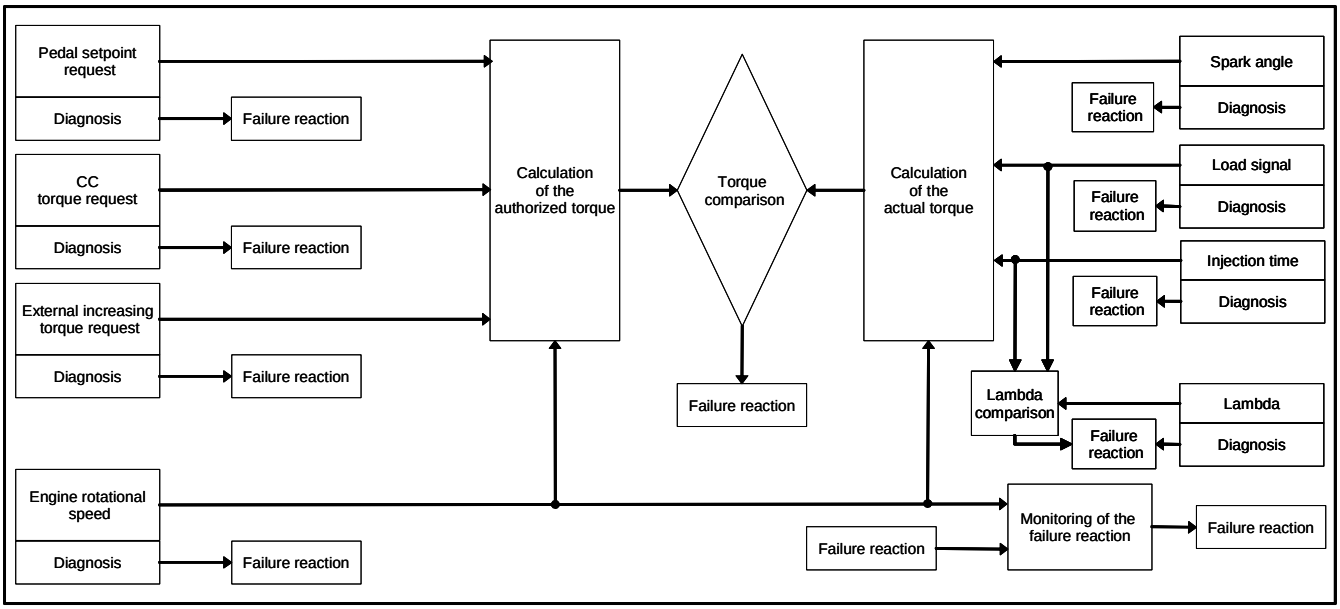


Figure 4 Level 2 function monitoring, gasoline manifold injection

EGAS_e-212 • Gasoline direct injection



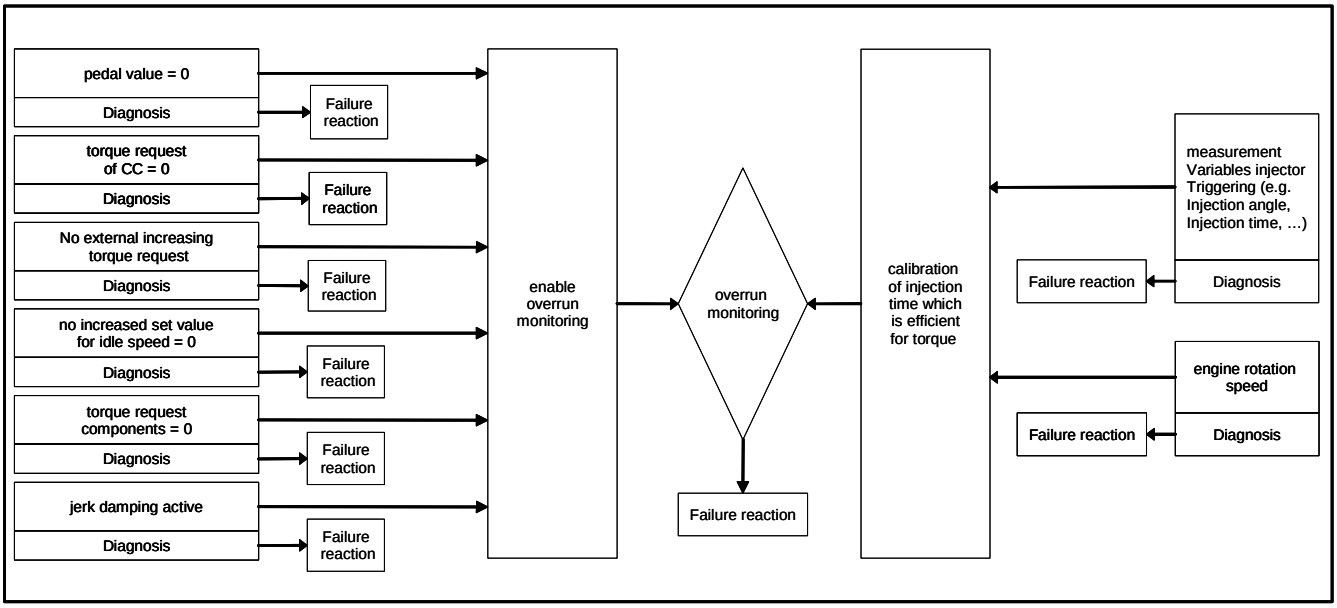
EGAS_e-213

Figure 5 Level 2 function monitoring, gasoline direct injection

EGAS_e-577 • **Monitoring Structures Diesel**

EGAS_e-578 Diesel monitoring consists of overrun monitoring and acceleration comparison or overrun monitoring and torque comparison.

EGAS_e-214 → Diesel (overrun monitoring)



EGAS_e-215

Figure 6 Level 2 function monitoring, Diesel / continuous torque monitoring (overrun monitoring)

EGAS_e-217 → Diesel (acceleration comparison)

EGAS_e-218

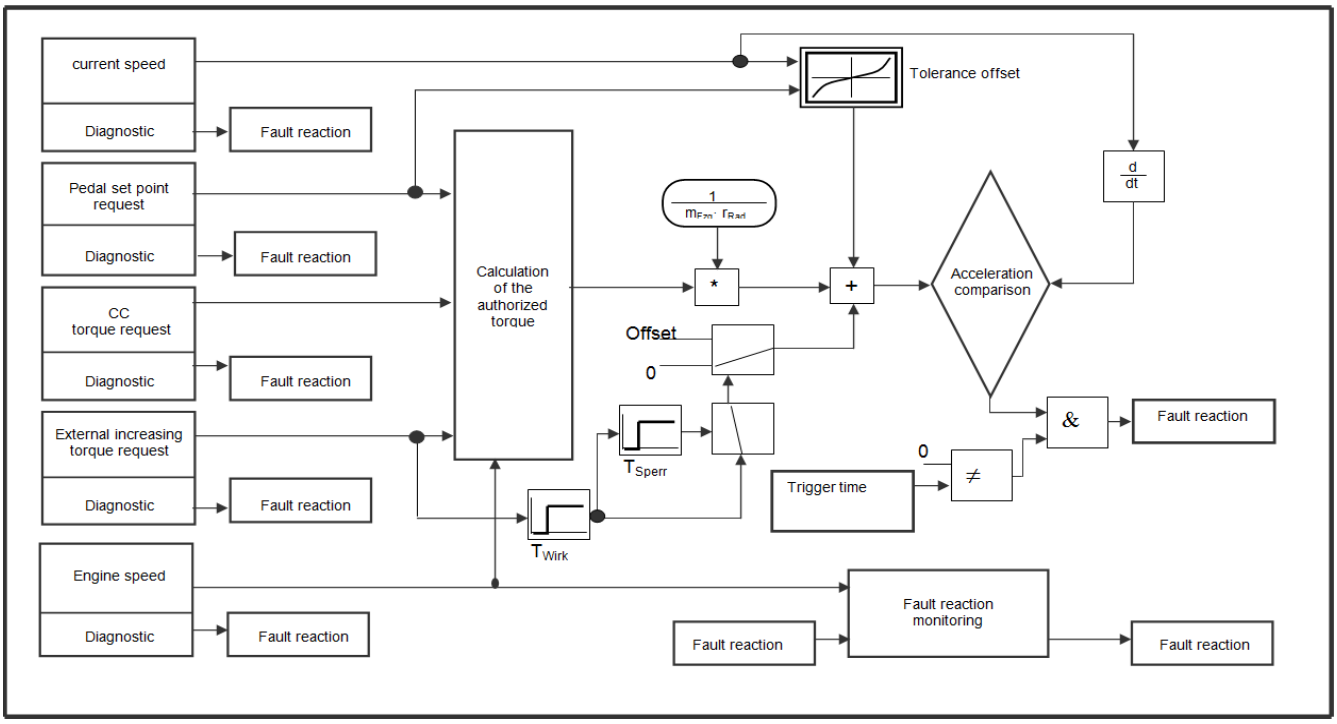


Figure 7 Level 2 function monitoring, diesel / continuous torque monitoring (acceleration comparison)

EGAS_e-579 → Diesel continuous torque monitoring (torque comparison)

EGAS_e-216

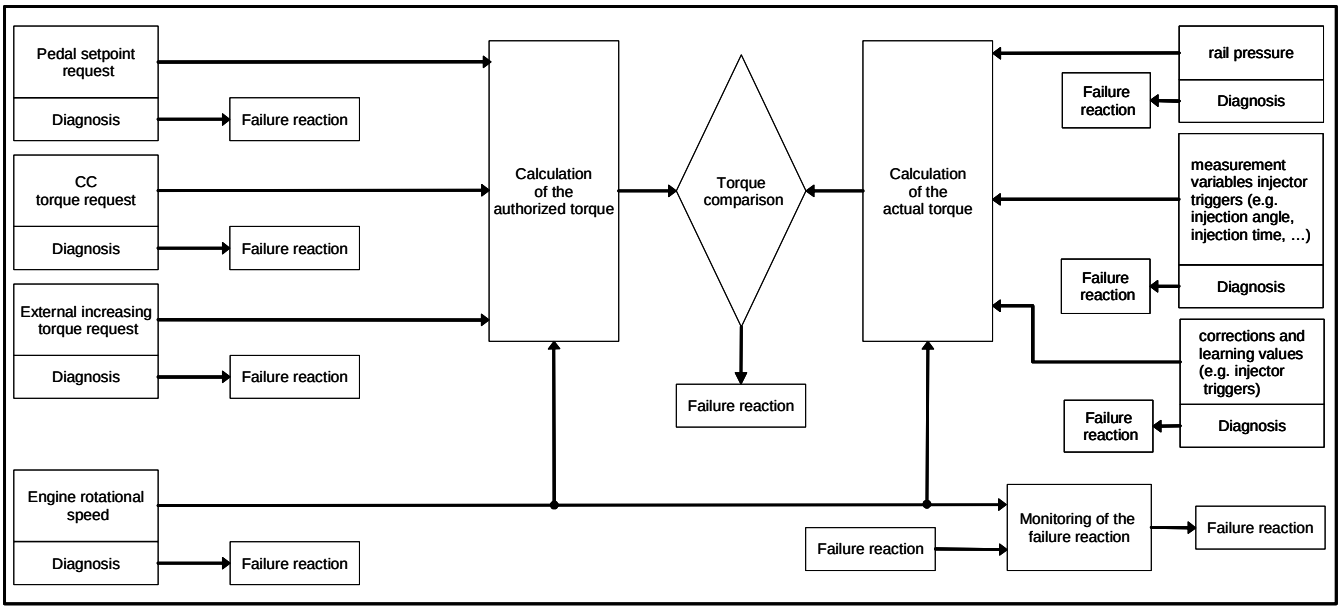


Figure 8 Level 2 function monitoring , Diesel / continuous torque monitoring (torque comparison)

EGAS_e-219 **The following tables contains the detailed monitoring tasks of level 2:**

EGAS_e-220 **Signals paths of ECUs which are network integrated:**

EGAS_e-221	Content of the transmitted scopes with monitoring relevance [1])	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-222	Vehicle acceleration, if applicable calculated from vehicle speed (Error coverage of currentness + signal transmission)	Diesel-Acceleration Monitoring

EGAS_e-224 **Validation of incoming parameters in level 2:**

EGAS_e-225	•Accelerator pedal [2])	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-226	•Brake [2])	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-227	•External and torque increasing requests 2)	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-228	•Air mass (as main load signal)	Gasoline-Manifold Injection Gasoline-Direct Injection

EGAS_e-229	•Intake manifold pressure (as main load signal)	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-230	•Fuel mass	Gasoline-Direct Injection
EGAS_e-231	•Engine speed	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-232	•Spark angle	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-233	•Injection time duration	Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-234	•Injection control variables (e.g. startup trigger)	Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-235	•Lambda	Gasoline-Direct Injection

EGAS_e-223 [1)] *may be required in the future*

EGAS_e-236 [2)] *„raw signals" at the control unit, ref. chapter definitions of terms*

EGAS_e-237 [3)] *During overrun*

EGAS_e-238 **Function Monitoring**

EGAS_e-239	•Torque comparison (permissible torque with current torque)	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-240	•Overrun monitoring	Diesel-Torque Monitoring Diesel-Acceleration Monitoring

EGAS_e-241	•Shutoff path test (up to actuator output stage)	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-242	•System reaction (injection cut off) of level 1 due to a failure case 4)	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-243	•A/D converter check	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-244	•Plausibility of torque loss from level 1	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-245	•Plausibility of adaption-/ correction values from level 1	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-246	•Cancel cruise control by brake request(internal cruise control)	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring

EGAS_e-247	•Monitoring of the brake overrun function	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-248	•Acceleration comparison	Diesel-Acceleration Monitoring

EGAS_e-249 *4) for fault reactions, which cannot be implemented in level 2*

EGAS_e-250 *5) project specific determination valid for gasoline intake manifold injection and direct injection*

EGAS_e-251 **Reactions in case of fault (fault-specific)**:

EGAS_e-252	•Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-253	•Actuator output stage switch-off	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-254	•Power limited limp home mode (e.g. Injection cut off)	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring

EGAS_e-255 **10.1.3.1 Inclusion of the torque loss of level 1 for "permissible torque" calculation**

EGAS_e-256 If using a target loss torque from level 1 for calculation of the permissible torque in level 2, the value shall be validated in level 2. fault reaction ref. appendix.

EGAS_e-257 **10.1.3.2 Taking over Adaptation Values / Correction Factors from Level 1 to Level 2 (Tolerance limitation)**

EGAS_e-258 If adaptation values and/or correction values with torque effect shall be transferred from level 1 to level 2, they shall be checked to be compliant with permissible limits. fault reaction ref. appendix.

EGAS_e-259

10.1.3.3 Monitoring of the Injection Output Variables from Level 1

EGAS_e-260 Function:

Plausibility of the controlled variables in level 2

EGAS_e-261 The measured injection time durations which are available in level 2 shall be checked value specific to be compliant with plausible limits.

EGAS_e-262 Examples:

EGAS_e-263
- plausible injection angle ranges

EGAS_e-264
- Adherence to maximum number of cylinders

EGAS_e-265
- injection type within maximum injection type number

EGAS_e-266 In case of invalid deviations, it shall be presumed an existing fault in level 1.

EGAS_e-267 fault reaction ref. appendix.

EGAS_e-268

10.1.3.4 Monitoring of the Trigger Output Unit (e.g. TPU, PCP)

Function:

EGAS_e-269 Comparison of the setpoint output control values from level 1 with the measured current values in level 2.

EGAS_e-270 For detection e.g. of toggled or defective RAM cells of the control output unit, the measured current values in level 2 for the injector drivers shall be checked to be plausible with the setpoint output control values of level 1.

EGAS_e-271 For each calculating cycle in level 2 at least one cylinder (e.g. with rotating cylinder pointer) shall be checked.

EGAS_e-272 With appropriate measures it shall be ensured that invalid copies of input values into the output memory are detected.

EGAS_e-273 Fault reaction, ref. to appendix.

EGAS_e-274

10.1.3.5 Continuous Torque Monitoring Diesel (Torque Comparison), Reverse Calculation of Current Torque Level 2

EGAS_e-275 The injection output variables calculated in level 1 are converted into electrical trigger signals by a trigger output unit (e.g. TPU, PCP).

EGAS_e-276 For reverse calculation of the current torque the electrical trigger signals of the trigger circuits are measured event depending. After transformation into time-, angle- and cylinder depending measurement data they are given as input variables of level 2.

EGAS_e-277 For more reverse calculation of torque the injection relevant and engine speed synchronous rail pressure shall be used.

EGAS_e-278 The requirements for validate the input value shall be described in the next chapter.

EGAS_e-279

10.1.3.5.1 Rail Pressure Monitoring

EGAS_e-280

10.1.3.5.1.1 Level 1 Requirements

EGAS_e-281 The rail pressure diagnostic shall be defined project specific.

EGAS_e-282 For monitoring purposes for single channel rail pressure capturing systems the following minimum plausibility's shall be regarded:

EGAS_e-283 • SRC high / low diagnostic

EGAS_e-284 • Rail pressure gradient diagnostic (direction specific)

EGAS_e-285 ***10.1.3.5.1.2 Interface Signals of Level 2***

EGAS_e-286 Detected faults shall be provided to level 2 with the diagnostic status.

EGAS_e-287 For validation of rail pressure in level 2 the values of the rail pressure gradient with their corresponding diagnostic status shall be provided to level 2.

EGAS_e-288 ***10.1.3.5.1.2.1 Limp-Home Mode***

EGAS_e-289 In case of a detected fault it shall be switched into a limp-home mode by using rail pressure setpoint as replacement value for the rail pressure controller.

EGAS_e-290 In the reverse calculation for the current torque in level 2 it shall be switched to the replacement value simultaneously.

EGAS_e-291 ***10.1.3.5.1.3 Level 2 Requirements***

EGAS_e-292 The raw value of the rail pressure sensor shall be used in level 2.

EGAS_e-293 ***10.1.3.5.1.3.1 Plausibilities***

EGAS_e-294 In analogy to level 1 for single channel rail pressure capturing systems the following minimum scope shall be considered:

EGAS_e-295 • SRC high / low monitoring

EGAS_e-296 • monitoring of rail pressure gradient diagnostic of level 1

EGAS_e-297 The monitoring of the rail pressure gradient diagnostic checks if an fault is detected in level 1 due to exceeding/ being below a limit value.

EGAS_e-298 In case of a fault detection the selection of limp-home mode depends on whether in level 1 a fault has been detected or not (ref. following description).

EGAS_e-299 ***10.1.3.5.1.3.2 Limp-Home Mode when a Failure was detected in Level 1***

EGAS_e-300 For more reverse calculation of the current torque in level 2 the rail pressure setpoint for the rail pressure control shall be used.

EGAS_e-301 ***10.1.3.5.1.3.3 Limp-Home Mode when a Failure was not detected in Level 1***

EGAS_e-302 A fault exists in level 1.

EGAS_e-303 The rail pressure information is not reliably available any more.

EGAS_e-304 Fault reaction ref. appendix.

EGAS_e-305 ***10.1.3.5.2 Torque Relevant Efficiencies of Injection Quantities***

EGAS_e-306 If injection quantities get weighted with efficiency factors from level 1 for the determination of torque calculations, these efficiency factors have to be validated in level 2. fault reaction ref. appendix.

EGAS_e-307 ***10.1.3.5.3 More Torque Relevant Efficiencies (e.g. Air Influence)***

EGAS_e-308 Additional physical parameters may affect to the accuracy in reverse calculation of the current torque in the system. These may be further efficiency factors for the relevant fuel injections. If these parameters shall be used from level 1 they have to be validated in level 2.

EGAS_e-309

10.1.3.6 Continuous Diesel Monitoring (Acceleration Comparison)

EGAS_e-310 Optional to the “continuous torque monitoring” for diesel, the continuous acceleration monitoring may be realized.

EGAS_e-311

10.1.3.6.1 Level 1 Requirements

EGAS_e-312 Basic principle:

EGAS_e-313 1. The drivers` input is interpreted as vehicle target acceleration.

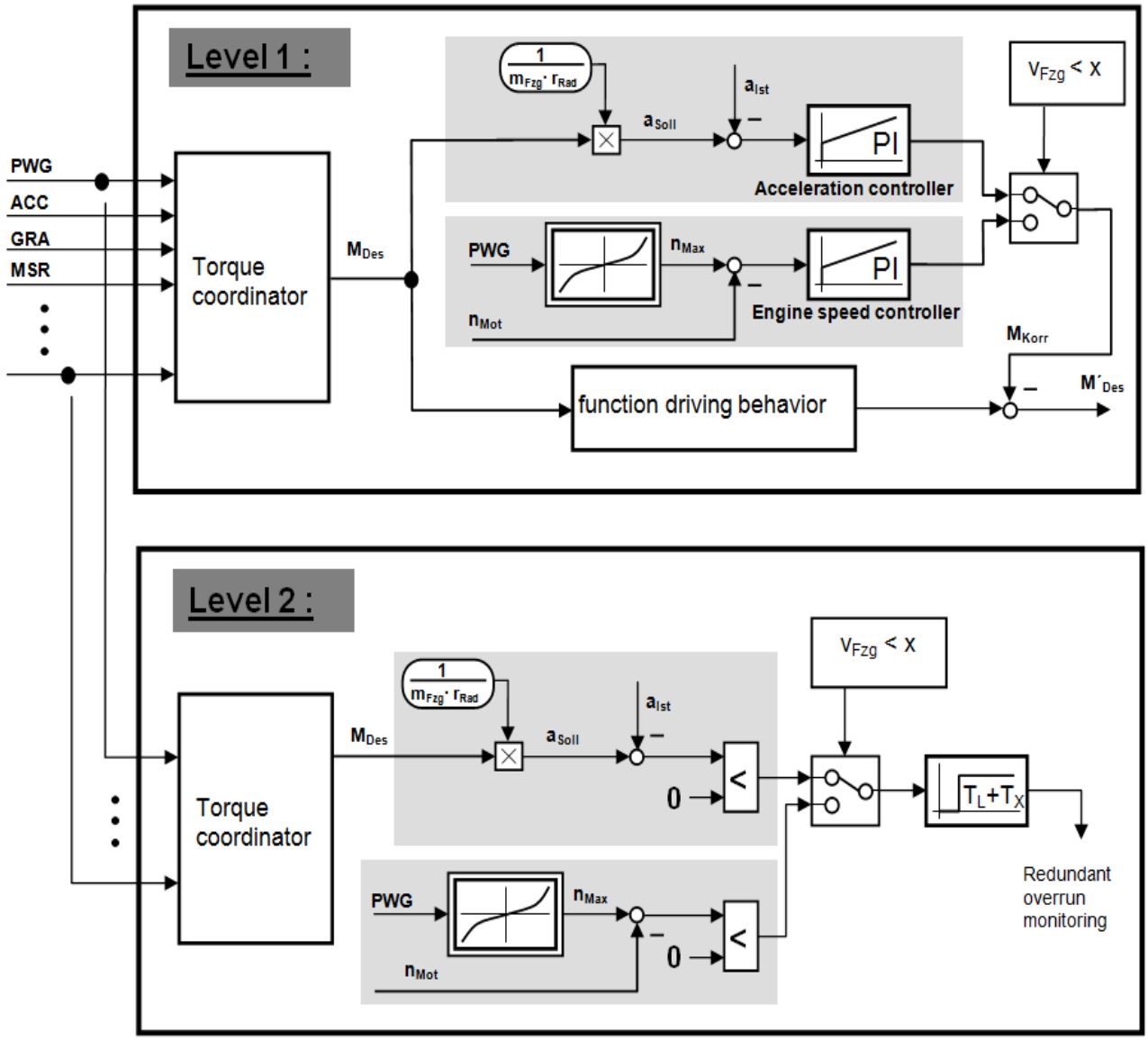
EGAS_e-314 2. When exceeding this target acceleration, an acceleration based driving behaviour shall be activated.

EGAS_e-315 Description:

EGAS_e-316 Based on the target engine torque, the vehicle target acceleration shall be calculated, by using the power train transmission ratio and additional vehicle parameters (e.g. vehicle reference mass, reference air drag coefficient (C_d value), etc.)

EGAS_e-317 The commanded engine torque shall be reduced by using a regulator if the current vehicle acceleration exceeds the setpoint vehicle acceleration.

EGAS_e-318 This regulator shall be implemented in parallel to the torque path and it is limited downwards to 0 Nm indicated torque (fig. 9).



EGAS_e-319

Figure 7 Diesel / continuous monitoring (acceleration comparison), overview

EGAS_e-320 Below a calibrateable vehicle speed threshold, the acceleration regulator is switched to an engine speed regulator.

EGAS_e-321 This Function in level 1 serves to ensure the drivability when exceeding the target vehicle acceleration. Thus, an unwanted intervention of level 2 (e.g. when driving downhill) is avoided.

EGAS_e-322 ***10.1.3.6.2 Level 2 Requirements***

EGAS_e-323 In level 2 (fig. 8), based on redundantly captured input signals, the current vehicle acceleration as well as the engine speed shall be monitored.

EGAS_e-324 If the current vehicle acceleration for an calibrateable time is higher than the target acceleration, level 2 shall limit the driving torque to zero.

EGAS_e-325 Therefore the overrun monitoring shall be activated to detect a possible fault (ref. fig. 6).

EGAS_e-326 Additionally above to a calibrateable engine speed threshold, the idle speed controller and the torque loss compensation shall be deactivated.

EGAS_e-327 This ensures that the target torque of level 1 shall certainly be 0 Nm.

EGAS_e-328

10.1.3.7 Continuous Diesel Monitoring, Overrun Monitoring

EGAS_e-329 The overrun monitoring known from present diesel monitoring systems shall be integrated in the continuous torque-/acceleration monitoring as parallel monitoring path for the torque comparison.

EGAS_e-330 Fault reaction ref. appendix.

EGAS_e-331

10.1.4 Validation of the Torque Measurement in the ECU Network

EGAS_e-332 The validating of torque output variables in the ECU network shall be defined project specific.

EGAS_e-333

10.1.5 Level 3 Controller Monitoring

EGAS_e-334 Controller monitoring refers to the interaction between software and hardware structures. It enables the detection of faulty operations of the function controller (controller core, affected areas in RAM/ROM).

EGAS_e-335 In the function controller, the RAM/ROM storage components are normally monitored at least once per driving cycle (at initialization or previous power latch).

EGAS_e-336 If a fault is detected, the check shall be mandatory executed at the next initialization.

EGAS_e-337 Engine start (if software controlled) or combustion is allowed only after the check is completed without faults.

EGAS_e-338 **Level 3 consists of 2 basic elements:**

- EGAS_e-339 The physically independent monitoring module (L3_MM realized through separate hardware) communicates with the L3 monitoring software in the function controller (L3_SW in FC) via an interface.
- EGAS_e-340 The L3_MM asks one question cyclically to the L3_SW in the function controller FC from at least 10 different questions ; it monitors the reception of a cyclical test result, makes the assessment and in case of an fault initiates the fault reaction.
- EGAS_e-341 The monitoring module can be performed as an ASIC or as a controller.
- EGAS_e-342 When using the RAM/ROM components in L3_MM these components shall be cyclically tested at least once for each driving cycle.
- EGAS_e-343 The clock of the monitoring module shall be separately implemented from the main computer.
- EGAS_e-344 L3 monitoring software of the function controller (L3_SW in FC) shall communicate with the L3_MM via interface.
- EGAS_e-345 The interaction between L3_MM and L3_SW in FC is also described as question / answer communication
- EGAS_e-346 Several test paths shall be processed on the function controller (ref. to 10.1.5.3).
- EGAS_e-347 Each test path provides an exactly defined numerical partial result depending on the question.

EGAS_e-348 The combination of the partial results leads to a numerical total result (test result), which will be transmitted to the L3_MM by the communication interface.

- EGAS_e-349 The L3_SW in the FC signals the fault-free operation to the L3_MM by means of correct answers.

EGAS_e-350 (ref. to fig. 3)

EGAS_e-351

10.1.5.1 Monitoring of the Q&A Communication

EGAS_e-352

10.1.5.1.1 Monitoring with L3_MM

EGAS_e-353 The L3_MM expects an accurately defined answer from the L3_SW in the function controller within a defined time period.

EGAS_e-354 In case of a fault the L3_MM provides an internal error counter and repeats the falsely answered question.

EGAS_e-355 If the error counters end is reached, the monitoring module shall switch off the actuator power output stages and triggers a limited number of SW resets by the function controller to increase the availability.

EGAS_e-356 If the L3_MM receives an answer at the false moment, the same fault reaction shall be performed.

EGAS_e-357 The error counter processing in the L3_MM shall be designed so that fault detection states lead to a faster reaching of fault reaction threshold than to a detected fault-free state leading to „a error counter reset".

EGAS_e-358 The monitoring module shall not be subjected to development and modification cycles of a flash based control unit and shall be independent of the project or vehicle equipment.

EGAS_e-359 The questions generated by the monitoring module are generic and determined already during the definition of the engine control system.

EGAS_e-360 The adjustment to the project-specific characteristics shall be performed by means of unique parameters on the function controller's side.

EGAS_e-361

10.1.5.1.2 Monitoring with L3_SW of the Function Controller

EGAS_e-362 The L3_SW in the FC expects a new question from the L3_MM within a defined time period and checks the fault-free operation of the L3_MM.

EGAS_e-363 The test in the L3_SW in FC is initiated by the L3_SW in FC giving wrong answers at specific time intervals.

EGAS_e-364 The next error counter status transmitted in combination with the question from the L3_MM is checked by the L3_SW in the FC to see if the fault detection is reflected in the error counter modification.

EGAS_e-365 In case of a fault, the L3_SW in FC uses an internal error counter and transmits again a wrong answer to the L3_MM.

EGAS_e-366 If the error counters end is reached, the function controller switches off the actuator output stages and triggers a limited number of resets to increase the availability.

EGAS_e-367 (ref. to fig. 3)

EGAS_e-368

10.1.5.2 Iteration Rate of the Q&A Communication

EGAS_e-369 The iteration rate shall not exceed a limit value of 80 ms.

EGAS_e-370 This is required to guarantee sufficient quantification for the fault debouncing.

EGAS_e-371

10.1.5.3 Test Paths of the L3_SW of the Function Controller

EGAS_e-372 Independent test paths, which form a partial response of the L3_MM shall be differentiated :

EGAS_e-373

- Program flow check

EGAS_e-374 The program flow control shall verify if all monitored level 2 modules (including TPU, cyclic RAM/ROM tests) are processing in fixed timeslots and in the right sequence.

EGAS_e-375
- Function-specific instruction set test

EGAS_e-376 It enables the detection of faults in the controller core and execution of level 2 functions and shall be adapted to the validating relevant monitoring functions.

EGAS_e-377 To avoid disturbing the level 2 processes, a copy of the validation relevant contents or a comparable instruction set sequence shall be stored in separate RAM and ROM areas.

EGAS_e-378 With these, the level 2 test questions are representatively answered.

EGAS_e-379 All selected test data shall represent fictitious level 1 fault states and shall generate a corresponding part of the answer..

EGAS_e-380 The functionality of all validation relevant controller instructions of the copied content shall be tested.

EGAS_e-381 An automatic-generated instruction set is also permitted if it covers at least all instructions which are used in the monitoring of level 2 and 3.

EGAS_e-382

10.1.5.4 Question Generating of the Monitoring Module L3_MM

EGAS_e-383 The amount of questions and the quality of the corresponding input data sets for the function-specific instruction set test shall be defined in a manner so that a comprehensive fault detection is possible (10 questions at least).

EGAS_e-384 The monitoring module L3_MM selects a pre-determined set of different questions that are submitted to the function controller.

EGAS_e-385 By applying a pseudo random sequence, the interval between same questions is reduced (which means no pure random sequence). Through this, processing time for all determined questions is also limited.

EGAS_e-386

10.1.5.5 TPU Monitoring

EGAS_e-387 TPU`s or other comparable hardware components that are capable of operating independently and can have influence on safety relevant signals, are to be included into the monitoring concept of the function controller.

EGAS_e-388 The goal of monitoring is detecting the following faults:

EGAS_e-389
- Destroyed cells in the internal parameter memory

EGAS_e-390
- Data flow conflicts of systems with shared memory.

EGAS_e-391
- Non-plausibility in TPU calculation variables

EGAS_e-392
- The monitoring characteristics are:

EGAS_e-393
- Writeability test of the parameter memory (e.g. TPU- internal parameter RAM)

EGAS_e-394
- Program memory storage test (e.g. TPU program RAM cyclically, ROM once per driving cycle)

EGAS_e-395
- TPU monitoring is included in program flow checking.

EGAS_e-396
- Plausibility check of TPU characteristic calculation variables in the function controller (e.g. plausibility check of the engine speed calculation in the TPU by assessing separate segment interrupt times)

EGAS_e-397
- fault reaction

EGAS_e-398
- In case of fault, a reset is triggered in the function controller.

EGAS_e-399
10.1.5.6 Shutoff Path Test

EGAS_e-400
- Goal of the Monitoring

EGAS_e-401
- Check the shutoff paths to the power determining output stages, so that a safe shutoff is guaranteed in case of a fault.

EGAS_e-402
- Monitoring characteristics:
- One test per driving cycle

EGAS_e-403
- Remark : if the test is performed during power latch and no positive results were obtained, a new test shall be performed mandatory during the next initialization phase.

EGAS_e-404
- Engine run is authorized only after one successful shutoff path test per controller.

EGAS_e-405
- Fault reaction:

EGAS_e-406
- Reset until engine run authorization
- (ref. to 10.1.5.8 System reset behavior)

EGAS_e-407
10.1.5.7 A/D Converter Test

EGAS_e-408
The A/D converter test shall cover three different fault possibilities. This is necessary if safety-relevant signals are read by the A/D converter.

EGAS_e-409
The next table contains a procedure to detect A/D converter faults that shall be applied depending on the present system:

EGAS_e-410

Fault Indication	Idle-Speed Test Pulse Procedure on PVS2 Input*	ADC Channel (without V_{Ref})	2 separate A/D Converter in the System**
Gradient failure		x	x
Offset failure	x		x
Register Stuck (also MUX do not switch)	x		x

EGAS_e-411
** An optional channel shall be used for testing of non-analog PVS signals.*

EGAS_e-412
*** In this case an analog signal shall be read and compared with both A/D converter.*

The PVS2 signal shall be primary used.

EGAS_e-413
10.1.5.8 Reset System Behavior

EGAS_e-414
Effect:

EGAS_e-415
- The reset affects the monitoring module (MM) and the function controller (FC)

EGAS_e-416
- The power determining output stages are switched-off

EGAS_e-417
- The duration of the reset status shall be determined specifically for each project

EGAS_e-418
- Tests after reset:

EGAS_e-419
- The stored information regarding the cause of the SW reset shall be evaluated before the next engine start can be authorized.

EGAS_e-420
- e.g. if a RAM/ROM failure shall be detected, the complete monitored memory shall be checked before a new release is allowed.

EGAS_e-421
- If no other requirements has higher priority, the remaining RAM-/ROM area shall be checked and finished during the ongoing driving cycle.

EGAS_e-422
- The maximum valid number of SW resets in a driving cycle shall be specific defined for every project.

EGAS_e-423
- Afterwards the power-regulating output stages shall be switched off (currentless) until vehicle restart.

EGAS_e-424
- Restart after reset:

EGAS_e-425
- The synchronization between MM and FC shall be done via a defined sequence in the question / answer communication..

EGAS_e-426
- The control and test sequences for the MM and FC shutoff paths are coupled to the communication synchronization. The test delivers a result about the operating capability of both shutoff paths.

EGAS_e-427
- The power determining output stages are released after a successful test.

EGAS_e-428

10.1.5.9 Diagram of the Level 3 Fault Reactions

Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS working group

EGAS_e-429

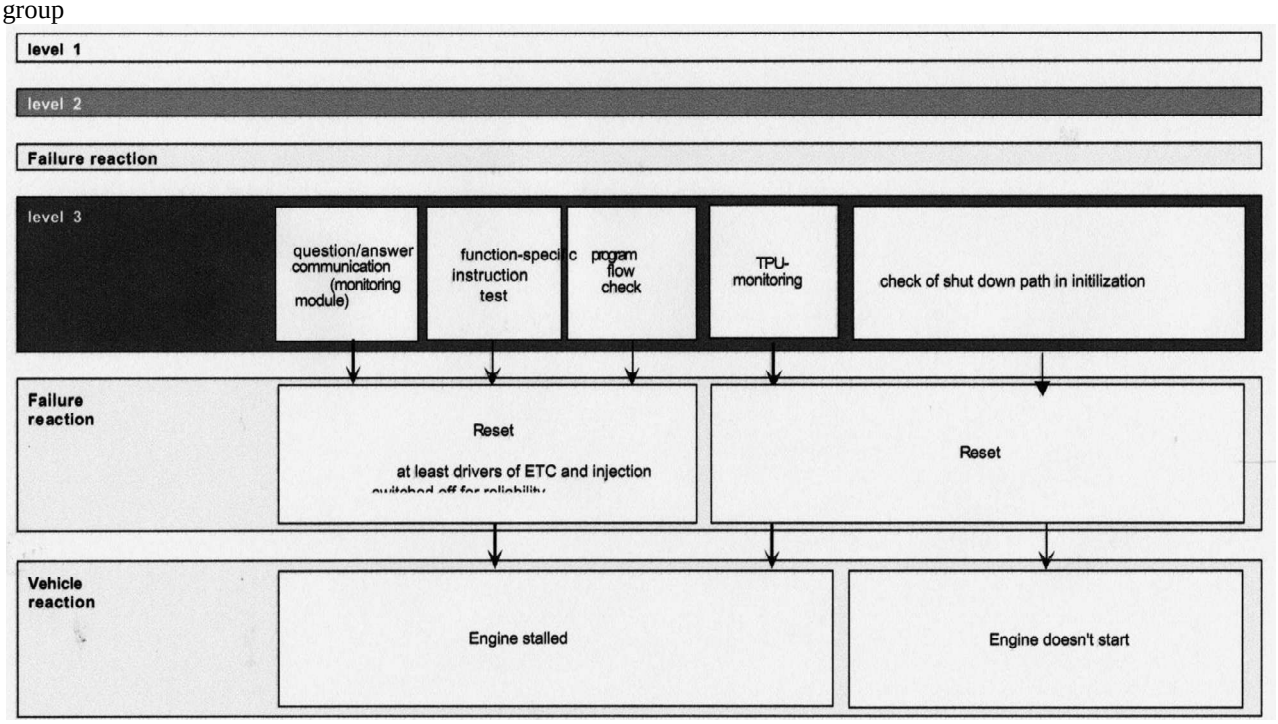


Figure 8 Level 3 controller monitoring fault reactions, gasoline and diesel

Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS working group

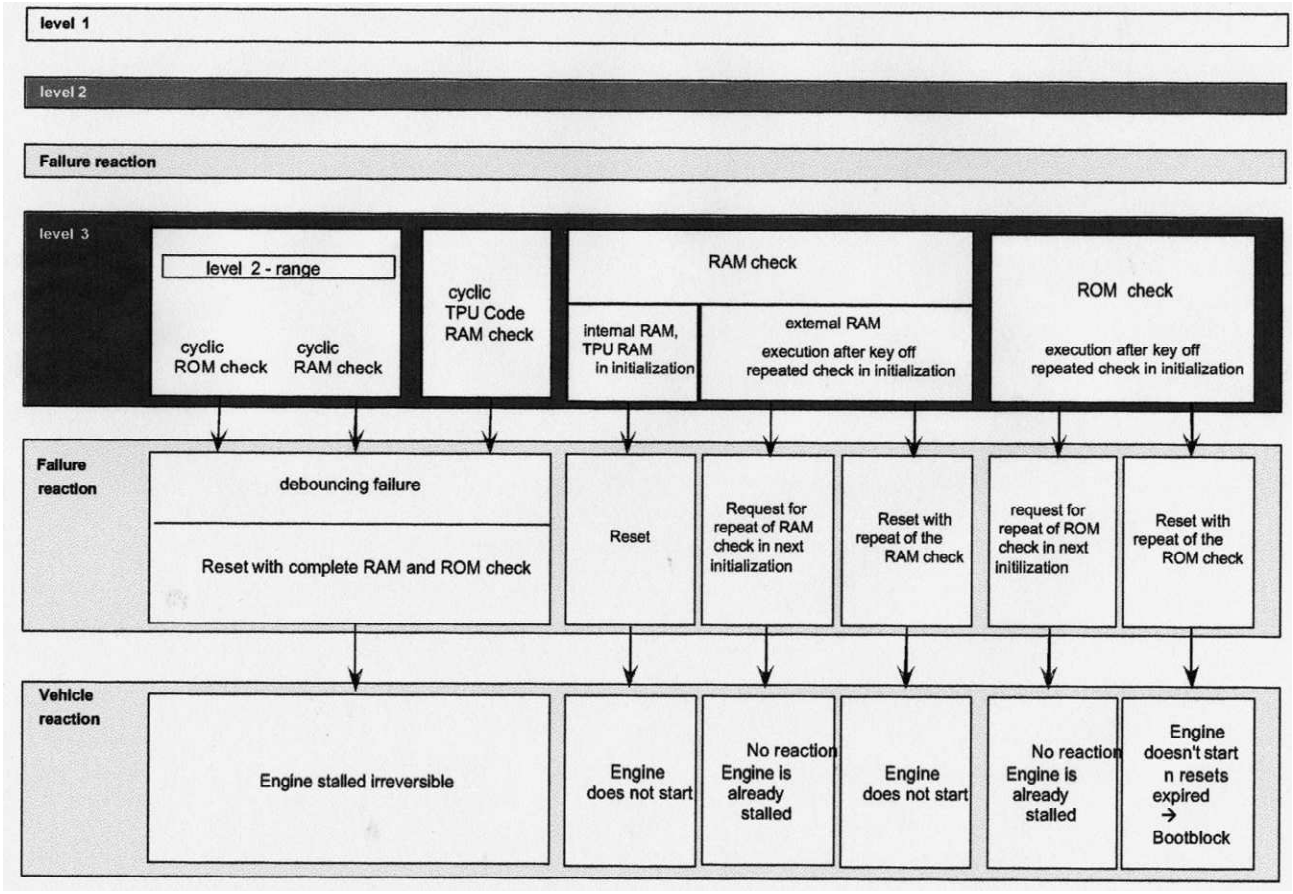

level 1
level 2
Failure reaction
level 3
level 2 - range
cyclic ROM check
cyclic RAM check
cyclic TPU Code RAM check
RAM check
internal RAM, TPU RAM in initialization
external RAM
execution after key off repeated check in initialization
ROM check
execution after key off repeated check in initialization
Failure reaction
debouncing failure
Reset with complete RAM and ROM check
Reset
Request for repeat of RAM check in next initialization
Reset with repeat of the RAM check
request for repeat of ROM check in next initilization
Reset with repeat of the ROM check
Vehicle reaction
Engine stalled irreversible
Engine does not start
No reaction Engine is already stalled
Engine does not start
No reaction Engine is already stalled
Engine doesn't start n resets expired → Bootblock

Figure 9 Level 3 memory test fault reactions: gasoline and diesel

EGAS_e-430

EGAS_e-431

10.2 System Fault Reactions

EGAS_e-432 The following principles shall be considered for the fault reactions:

EGAS_e-433 • Necessary plausibility tolerances depend on OEM specific project requirements.

EGAS_e-434 • If throttle limp-home is requested and throttle limp-home position is not reached, ICO shall be activated (gasoline).

EGAS_e-435 • The max. duration at fault detection until start of the system reaction shall be defined fault specific.

(e.g. benchmark for torque monitoring = 500 ms)

EGAS_e-436 • The detection of certain faults in level 2 leads to the activation of ICO directly or indirectly by the torque comparison or acceleration comparison (gasoline / diesel).

EGAS_e-437 Refer to detailed tables of fault reactions in appendix.

EGAS_e-438

10.3 Additional Technical Requirements

EGAS_e-439

10.3.1 Safe Engine Stop

EGAS_e-440 Shut-off of the combustion engine with ignition key (T 15) off.

The combustion engine shall be stalled reliably within a permissible time delay,

EGAS_e-441 if ignition key off (T15 = off) is detected.

This shall be ensured due to a shut-off path in the control unit, independently from the (main) controller.

Appropriate measures: e.g. disabling of ignition, fueling device or fuel injectors, fuel pump etc.

EGAS_e-442 Other comparable implementations are to be agreed with the OEM.

EGAS_e-443

11 Appendix: Fault Reactions

EGAS_e-444

11.1 Level 1 Monitoring Faults

EGAS_e-445

11.1.1 Pedal Value Sensor

EGAS_e-446	**Fault description:** nominal value 1 > threshold (signal-range-check high)	
EGAS_e-447	Limp home mode with PVS2. Additional restrictions: limitation of max. value and max. gradient, if brake active / brake signal fault detected, demand of idle speed.	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-448	**Fault description:** nominal value 1 < threshold (signal-range-check low)	
EGAS_e-449	Limp home mode with PVS2. Additional restrictions: limitation of max. value and max. gradient, if brake active / brake signal fault detected, demand of idle speed.	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-450	**Fault description:** nominal value 2 > threshold (signal-range-check high)	
EGAS_e-451	Limp home mode with PVS1. Additional restrictions: limitation of max. value and max. gradient, if brake active / brake signal fault detected, demand of idle speed.	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-452	**Fault description:** nominal value 2 < threshold (signal-range-check low)	

EGAS_e-453	Limp home mode with PVS1. Additional restrictions: limitation of max. value and max. gradient, if brake active / brake signal fault detected, demand of idle speed.	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-454	**Fault description:** Non-plausibility between nominal value 1 and nominal value 2 |nominal value 1 - nominal value 2| > threshold	
EGAS_e-455	Limp home mode with minimum value of PVS1 and PVS2. Additional restrictions: limitation of max. value and max. gradient, if brake active / brake signal fault detected, demand of idle speed.	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-456	**Fault description:** Power supply of PVS is beyond the authorized range (only for systems with one power supply line)	
EGAS_e-457	Idle speed demand	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-458	**Fault description:** Limp home mode with nominal value 1 and fault detection nominal value 1 > threshold (signal-range-check high)	
EGAS_e-459	Idle speed demand	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-460	**Fault description:** Limp home mode with nominal value 2 and fault detection nominal value 2 > threshold (signal-range-check high)	
EGAS_e-461	Idle speed demand	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-462	**Fault description:** Limp home mode with nominal value 1 and fault detection nominal value 1 < threshold (signal-range-check low)	

EGAS_e-463	Idle speed demand	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-464	**Fault description:** Limp home mode with nominal value 2 and fault detection nominal value 2 < threshold (signal-range-check low)	
EGAS_e-465	Idle speed demand	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring

EGAS_e-466 **Electro-Mechanical Actuating System (Gasoline with one Throttle-Valve Actuator)**

EGAS_e-467 Depending on the project it shall be performed a replacement value TVDV (Throttle Valve Default Value) for the throttle position sensor (e.g. : from air flow / intake manifold pressure, engine rotational speed)

EGAS_e-468	**Fault description:** TPS 1 > threshold (signal-range-check high)	
EGAS_e-469	Limp home mode with TPS2 and comparison with TVDV. The max. TPS shall be limited as a function of current engine speed.	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-470	**Fault description:** TPS 1 < threshold (signal-range-check low)	
EGAS_e-471	Limp home mode with TPS 2 and comparison with TVDV. The max. TPS 2 shall be limited as a function of current engine speed.	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-472	**Fault description:** TPS 2 > threshold (signal-range-check high)	
EGAS_e-473	Limp home mode with TPS 1 and comparison with TVDV. The max. TPS 1 shall be limited as a function of current engine speed.	Gasoline-Manifold Injection Gasoline-Direct Injection

EGAS_e-474	**Fault description:** TPS 2 < threshold (signal-range-check low)	
EGAS_e-475	Limp home mode with TPS 1 and comparison with TVDV. The max. TPS 1 shall be limited as a function of current engine speed.	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-476	**Fault description:** TPS 1 + TPS 2 > threshold and TPS 2 plausible with TVDV	
EGAS_e-477	Limp home mode with TPS 2 and comparison with TVDV. The max. TPS 2 shall be limited as a function of current engine speed.	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-478	**Fault description:** TPS 1 + TPS 2 > threshold and TPS 1 and TPS 2 are not plausible with TVDV	
EGAS_e-479	Irreversible ICO of level 1, throttle actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-480	**Fault description:** TPS 1 + TPS 2 > threshold and TPS 1 plausible with TVDV	
EGAS_e-481	Limp home mode with TPS 1 and comparison with TVDV - the max. TPS 1 is limited as a function of the engine speed	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-482	**Fault description:** Limp home mode with TPS 1 and plausibilisation with TVDV and an additional fault is detected: TPS 1 < threshold or TPS 1 > threshold	
EGAS_e-483	Irreversible ICO of level 1, throttle actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-484	**Fault description:** Limp home mode with TPS 2 and plausibilisation with TVDV and an additional fault is detected: TPS 2 < threshold or TPS 2 > threshold	

EGAS_e-485	Irreversible ICO of level 1, throttle actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-486	**Fault description:** Limp home mode with TPS 1 or TPS 2 and plausibilisation with TVDV is active. In addition a load sensor fault occurs.	
EGAS_e-487	Irreversible ICO of level 1, throttle actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-488	**Fault description:** Throttle position regulator fault (Target / current value comparison) due to e.g. wrong setpoint demand or mechanical stucking throttle valve.	
EGAS_e-489	Irreversible ICO of level 1, throttle actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-492	**Fault description:** Output stage fault	
EGAS_e-493	Irreversible ICO of level 1, throttle actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection

EGAS_e-494 **Monitoring of External Requests**

EGAS_e-495	**Fault description:** Faulty / missing message for external torque request (detection in level 1)	
EGAS_e-496	Inhibition of the request, customer-specific reversible or irreversible, customer-specific torque transition function	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring

EGAS_e-497 **Monitoring of Programming and Power Supply**

EGAS_e-498	**Fault description:** Flash : programming not finished	
EGAS_e-499	Remain in boot block	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring

EGAS_e-500	**Fault description:** Flash : programming fault	
EGAS_e-501	Remain in boot block	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-502	**Fault description:** Power supply outside specification	
EGAS_e-503	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring

EGAS_e-504 **Brake Information**

EGAS_e-505	**Fault description:** Non-plausibility of the redundant brake signals	
EGAS_e-506	Switch off CC	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-507	**Level 2 Faults of the Functional Monitoring**	
EGAS_e-508	**Fault description:** Faulty / missing message for external torque increasing requests (EDC, transmission, etc.) (detection in level 2)	
EGAS_e-509	Reaction analog to "faulty / missing message for external torque request (detection in level 1)"	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-510	Faulty engine speed; Deviation between level 1 and level 2 (detection in level 2)	

EGAS_e-511	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-512	**Fault description:** Fault detection of driver's request; Deviation between level 1 and level 2. (detection in level 2)	
EGAS_e-513	After a calibrateable number of resets and no fault healing, request / monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Acceleration Monitoring
EGAS_e-514	After a calibrateable number of resets and no fault healing, request / monitor irreversible ICO command from L2	Diesel-Torque Monitoring
EGAS_e-515	**Fault description:** Faulty switch-off or non-permitted activation of the cruise control (detection in level 2)	
EGAS_e-516	Disable CC request; if disabling not possible : request / monitor torque comparison, irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-517	Disable CC request : if disabling not possible : request / monitor torque comparison, irreversible ICO command from L2	Diesel-Torque Monitoring
EGAS_e-573	Disable CC request : if disabling not possible : request / monitor acceleration comparison, irreversible ICO command from L2	Diesel-Acceleration Monitoring
EGAS_e-518	**Fault description:** Faulty signals of fuel mass, oxygen sensor, load (detection in level 2)	
EGAS_e-519	Plausibility in level 2 only in lean fuel operation mode ; irreversible disabling of the lean fuel operation mode, transition to homogenous fuel operation mode.	Gasoline-Direct Injection
EGAS_e-520	**Fault description:** Faulty injection actuation time (detection in level 2)	
EGAS_e-521	Shift to homogenous fuel operation mode	Gasoline-Direct Injection
EGAS_e-522	After a calibrateable number of resets and no fault healing, request / monitor irreversible ICO command from L2	Diesel-Torque Monitoring

EGAS_e-523	**Fault description:** faulty spark angle (detection in level 2)	
EGAS_e-524	After a calibrateable number of resets and no fault healing, request / monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-525	**Fault description:** Plausibility fault of the load signal with TPS (detection in level 2)	
EGAS_e-526	After a calibrateable number of resets and no fault healing, request / monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-527	**Fault description:** Fuel injection overrun monitoring: impermissible activation of injector controlling due to fault in level 1 during overrun at idle speed demand. (detection in level 2)	
EGAS_e-528	After a calibrateable number of resets and no fault healing, request / monitor irreversible ICO command from L2	Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-529	**Fault description:** Continuous torque monitoring / torque comparison: impermissible engine torque exceeding due to fault in level 1 (detection in level 2)	
EGAS_e-530	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-574	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring
EGAS_e-531	**Fault description:** ICO is not applied in level 1 (detection in level 2)	

EGAS_e-532	Shutdown of the power determining output stages	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-533	**Fault description:** A/D converter fault	
EGAS_e-534	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-535	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-536	Fault at torque loss from level 1 (detection in level 2)	
EGAS_e-537	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-538	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring
EGAS_e-539	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2 (only necessary at adequate compensation in level 1)	Diesel-Acceleration Monitoring
EGAS_e-540	**Fault description:** Plausibility fault of the current setpoint variables from level 1 in level 2 (detection in level 2)	
EGAS_e-541	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring Diesel-Acceleration Monitoring
EGAS_e-542	**Fault description:** Monitoring fault of the trigger output unit (TPU, PCP etc.) (detection in level 2)	
EGAS_e-543	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring Diesel-Acceleration Monitoring

EGAS_e-544	**Fault description:** fault at rail pressure monitoring (detection in level 2)	
EGAS_e-545	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring
EGAS_e-546	**Fault description:** fault when taking over of adaption values / correction factors from level 1 to level 2 (tolerance restriction); fault in path reverse calculation of current torque	
EGAS_e-547	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2, TV actuator currentless	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-548	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2	Diesel-Torque Monitoring
EGAS_e-549	**Fault description:** Fault when taking over of adaption values / correction factors from level 1 to level 2 (tolerance restriction); fault in path of calculation of permissible torque	
EGAS_e-550	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2; TV actuator currentless; or project specific fault reaction	Gasoline-Manifold Injection Gasoline-Direct Injection
EGAS_e-575	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2; or project specific fault reaction	Diesel-Torque Monitoring
EGAS_e-551	After a calibrateable number of resets and no fault healing, request/ monitor irreversible ICO command from L2; or project specific fault reaction (only necessary at adequate compensation in level 1)	Diesel-Acceleration Monitoring
EGAS_e-552	**Fault description:** Fault when taking over torque relevant efficiencies for injection quantities from level 1 (detection in level 2)	
EGAS_e-553	Demand on L1: Change to an operating mode without relevant efficiency	Diesel-Torque Monitoring
EGAS_e-554	**Fault description:** Continuous acceleration monitoring: Non-authorized acceleration upper deviation due to fault in level 1	
EGAS_e-555	Request / monitor irreversible ICO command from L2	Diesel-Acceleration Monitoring
EGAS_e-556	Acceleration- / V-signal acquisition incorrect	
EGAS_e-557	Switch to substitute v-signal from engine speed	Diesel-Acceleration Monitoring
EGAS_e-558	**Level 3 Faults of the Controller Monitoring**	

EGAS_e-559	**Fault description:** Time out fault or incorrect feedback of the error counter in the question / answer communication (detected by FC)	
EGAS_e-560	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-561	**Fault description:** Time out fault or incorrect answer in the question / answer communication (detection by MM)	
EGAS_e-562	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-563	**Fault description:** fault in the shutoff path test	
EGAS_e-564	Reset until engine operation is authorized	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-565	**Fault description:** fault in the non-volatile memory	
EGAS_e-566	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-567	**Fault description:** fault in the volatile memory	
EGAS_e-568	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring
EGAS_e-569	**Fault description:** fault in TPU monitoring	

EGAS_e-570	Reset	Gasoline-Manifold Injection Gasoline-Direct Injection Diesel-Torque Monitoring

12 List of Figures

Figure 1 Overview of the ETC system with interfaces (simplified example of a gasoline engine) 9
Figure 2 Safety block diagram 10
Figure 3 System overview; 3 level concept 13
Figure 4 Level 2 function monitoring, gasoline manifold injection 19
Figure 5 Level 2 function monitoring, gasoline direct injection 20
Figure 6 Level 2 function monitoring, Diesel / continuous torque monitoring (overrun monitoring) 20
Figure 9 Diesel / continuous monitoring (acceleration comparison), overview 29
Figure 10 Level 3 controller monitoring fault reactions, gasoline and diesel 34
Figure 11 Level 3 memory test fault reactions: gasoline and diesel 35